USS Abraham Lincoln CVN-72

USS ABRAHAM LINCOLN
Local Area Network
Management

Unclassifi

Agenda

- Pre-existing Conditions
- Road to Baseline
- Configuration Management
- Policies
- Future Plans
- Information Assurance

USS Abraham Lincoln CVN-72

Pre-Existing Conditions

Pre-Existing Conditions

- Network Management – No Baseline
  - Inadequate documentation for hardware/software configuration baseline
  - Addition of drops to the ISNS LAN without proper authorization
  - New drops not properly labeled and tagged
  - Installation of Non-Program of Record (POR) LinkSys and Cisco switches/hubs
  - Ship’s drawings out of date
  - Software and hardware installed not listed on the PPL/SSIL/CPL
  - Installed ready-service-spare blades in switches to expand network
  - Inaccurate hardware inventory

Pre-Existing Conditions

- Policies
  - Management policies non-existent or significantly out dated
- Training
  - Insufficient training for Division Officers, LCPOs, and LPOs on Network Management basics
  - Inadequate training path for switch maintainers and operators
  - Insufficient user training

USS Abraham Lincoln CVN-72

Configuration Management

Unclassifi

Road to Baseline

- Baseline process initiated in support of INSURV and scheduled COMPOSE upgrade
- Network switch/drop validation
  - Verified individual ports on every blade of every switch
  - Verified distant end location by cable tag for every drop
  - Compared results with drawings from multiple POR installations
  - Documented Non-POR drops
- Network hardware inventory validation
  - Identified/located all hubs and switches
  - Identified/located all computers and peripherals
  - Documented Non-POR hardware
- 12 month evolution to completion

Configuration Management

- LAN Expansion only authorized through the SHIPMAIN Ship Change Document (SCD) process.
  - CVN72 removed approximately 325 Non-POR network drops
  - CVN72 removed Non-POR hubs/switches

Configuration Management

- SHIPMAIN
  - Per PEO C4I SAN DIEGO CA (091745Z JAN 07), CVN 72 submitted SCD 5237 requesting POR documentation of 220 operationally required Non-POR network drops.
    - CNAF funded SCD updating last known set of network drawings from CY2000 to reflect current configuration
  - During dPIA 2006/07, only systems/programs with approved SCD's authorized to install on ABRAHAM LINCOLN

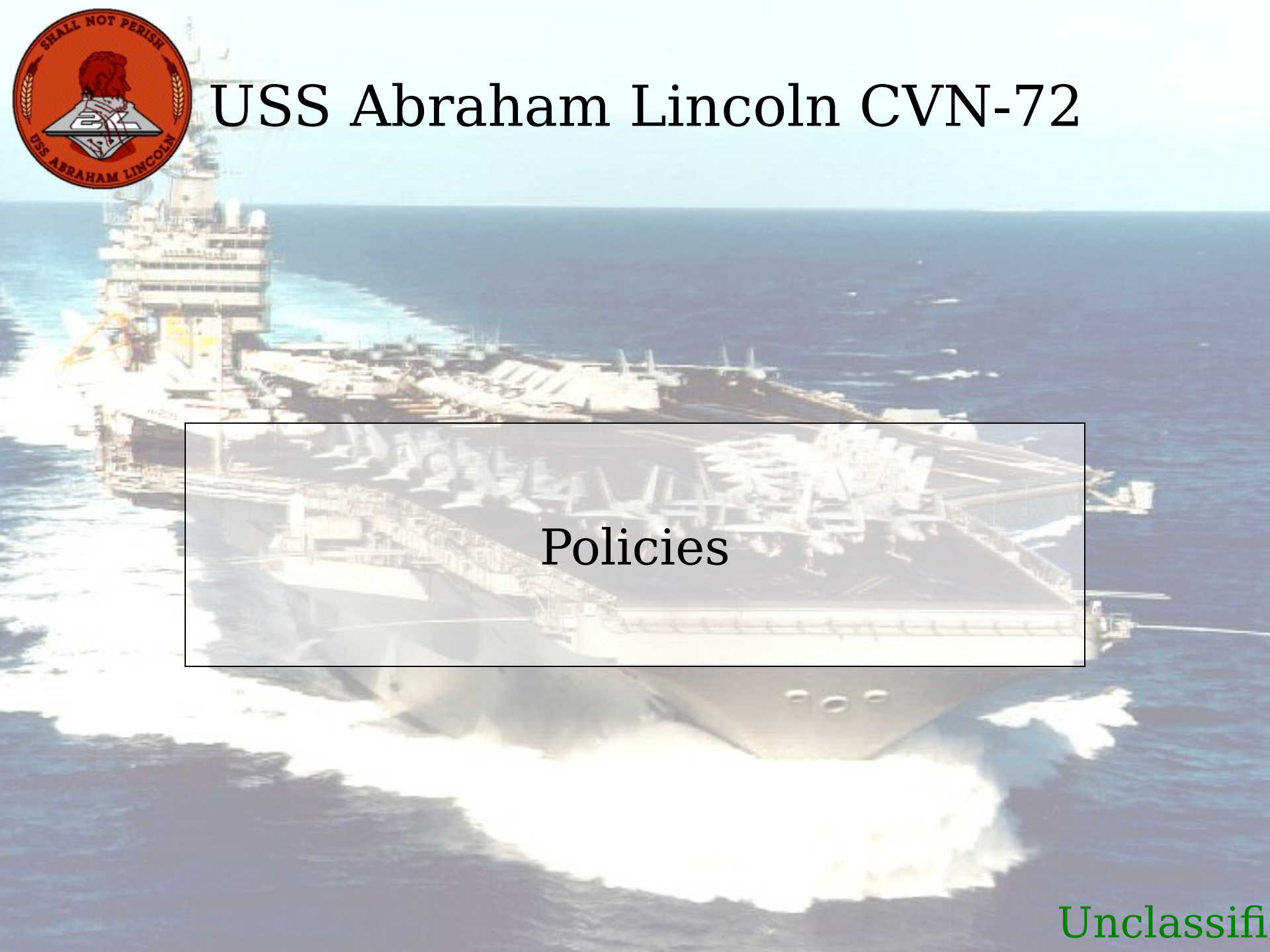
Configuration Management

- CVN72 has de-populated over crowded switches
  - Based on Alcatel 80% of individual switch capacity recommendations
  - Total virtual port capacity of a switch X 80%
  - Less 22 virtual ports for infrastructure support (switch dual homing to backbones)
  - Less 10 virtual ports held in reserve by ADP (populated by exception)
  - Total number of available ports per switch = 173
  - Note: each Omnistack added to a switch consumes 11 virtual ports

Combat Systems Configuration

- Software
  - COMPOSE installation baselined software configuration on CVN 72
  - Software authorized by PMW 160 via the PPL is installed on the CVN72 ISNS network
- Hardware
  - Hardware authorized by PMW 160 via the CPL is installed on the CVN72 ISNS network
- Integrated Systems/Non-ISNS Systems
  - Third Party Systems authorized by PMW 160 via the SSIL is installed on the CVN72 ISNS Network.
  - Third Party Systems are required to submit a current SSAA and IATO/ATO prior to installation.

USS Abraham Lincoln CVN-72



Policies

Combat Systems Network Policies

- Prior to IT support policy approval, the drafter must show:
  - Policy is enforceable
  - Policy is auditable
- Policies created and/or modified recently:
  - Set size limits on User Home Drive
  - Internet usage policies
  - Bandwidth management (Tier's)
  - Shared Drive standardization and access control
  - Exchange Server Mailbox and Public Folder management

Daily Reports

- Provides visibility of disk space utilization and critical operations
  - User Profile Directory
  - User Home Drive
  - Share Drive
  - Exchange Disk Space
  - Critical Backups
  - Targets Individual Accounts

IT Training

- Training, Training, Training
  - Take advantage of all training opportunities
  - Command will accept personnel shortages in customer service to support IT training
  - Individuals in the division pull “double-duty” when needed to support training opportunities
- Training opportunities ARE training requirements
  - Combat Systems proactive in obtaining IT training quotas

Our Keys to Success

- Maintaining standard configuration established by the Program Manager
- Establishing measurable and verifiable policies
- Routine audits
- Aggressive training
- Unrelenting, steadfast adherence to configuration management
  - Unauthorized LAN expansion
  - Installation of unapproved and untested software/hardware
  - Managing user expectations

Our Combination to Success

- Potentially unique CVN 72 Combat Systems leadership team (CSO, CSIO, CSMO) with strong backgrounds in:
  - Program Manager/SYSCOM, Fleet Commander, Combatant Commander and DOD policies, procedures and processes regarding Configuration Management and Information Assurance.
- CVN72 experience indicates that these skillsets are critical and recommends they are included in the C5I training pipeline prior to arrival on CVN.

USS Abraham Lincoln CVN-72

Concerns & Issues

ISNS Issues

- Aging Switches
  - Slow network performance
  - 80% of switch blades only support 10 MBPS ports.
- Ready Service Spares
  - PC warrantee support very good, but time late
  - At one point during deployment 30 desktops off line waiting for parts
  - On Board Spare for Server Parts.
- NMCI Integration
  - Shore elements (Air Wing, Embarked Staff)
  - NMCI workstations pose an inherent risk to CVN72 domain due to lack of ability to “push” IAVA and security patches

Required Assistance

- Asset Inventory
  - Require an automated tool to reduce manhours supporting audit.
- Spam Blockers
  - Require an automated tool to support email management.
- Anti-Spyware
  - Pest Control
  - Require an automated tool to support network security
- Network Attached Storage (NAS)
  - Lack of shipboard storage space
  - Include as authorized product on SSIL/CPL
- Intrusion Detection System (IDS)
  - Inadequate Training
  - Standard Fleet Wide PQS

Switch Issues

- Location
  - Geographic architecture of switches does not match user workspace density
  - Majority of the network drop requirements reside within workspaces in the proximity of the island structure
- Switch Cabinet
  - Switches often overheat due to lack of air flow
  - Switches should not be located where the general population can access the switches
  - Access to switches is problematic. During a power loss, operators are unable to reach switches before the UPS fails

PPL/SSIL/CPL (PSC) Issues

- Program Managers are not ensuring their products are included in the ISNS PPL/SSIL/CPL before distributing product to fleet users.
  - STELLA
  - EPSQ
  - PCEDVR
  - Netscape
  - DOD Sponsored Programs: PODCAST (Ipod)
- Falls behind commercial software version releases and lacks many common needed user applications
  - Adobe Professional
  - Internet Explorer
  - Microsoft Office Products (FrontPage, Project, Visio)
  - PDA Software (Hot Sync)
  - Blackberry

PPL/SSIL/CPL Issues

- The process to get software, hardware and systems on the PPL/SSIL/CPL is hard to achieve
  - Fleet units do not have the ability to conduct security and interoperability assessments
  - CVN 72 submitted 2 Network Change Requests (NCR) prior to dPIA (Sept ’06) in preparation for COMPOSE installation with no response to date.

Training and Management Issues

- No comprehensive LAN management policy published for afloat networks by CNAF/SPAWAR/NETWARCOM
- 3-day course needed to train afloat LAN managers on Configuration Management
  - User/Group Management
  - Information Management Policies
    - Web Page Content
    - Email Public Folders and Private Mailboxes
    - Bandwidth and File Server limitations/restrictions
  - Topology Management
  - Afloat Policies and Procedures
  - Expectation of users VS configuration management
- Funding source for civilian network operations certifications not identified (A+, Security +, CCNA, MCSE, etc)

File Server Size Issues

- File servers that support the user Home Drive and the Command Share Drive are 400 GB each.
  - CVN72 currently supports 3700 NIPRNET user accounts.
- Defrag utility needs 20% free space on file server to complete.
  - 80% of drive available for use (320 GB).
- Space available for user home drives (Z:)
  - 320/3700 = 0.0864GB = .864 MB per user
  - Users have less than 1 MB

File Server Size Issues

- Data transfer rate between the tape drive and the hard drive significantly decreased backup performance.
- To reduce the amount of time to save data, CVN72 has imposed stringent policies to restrict the amount of data that can be save to the user's Home Drive
  - Restrictions ensure that the file server supporting the user Home Drive server will not grow larger than 250 GB.

Uninterrupted Power Supplies (UPS)

- The edge switch UPS (APC-1400s)
  - At end-of-life requires replacing battery packs and UPS units
  - 1400-Models are no longer produced
- The ISNS Server UPS
  - Replaced all (4) UPS units (Clary SRN Series 2400VA) a year ago.
  - Replaced all (4) UPS battery packs during deployment.
- UPS do not “hold the load” for required PMS time of 9 minutes and only average approximately 4 minutes
- During a Network Forum at Everett Naval Station, the ISNS POR Managers reported that there are "known issues" with the ISNS UPS units.

Internal Networks

- Multiple CVN 72 departments manage non-ISNS networks
- Many departments (non-Combat Systems) receive insufficient system administration and network management training for non-ISNS networks
- No additional IT manning to support multiple non-ISNS networks
  - Support for non-ISNS networks provided by ISNS funded billets
  - Inadequate APL documentation or Planned Maintenance (PMS)
- Examples
  - Smart Carrier – Engineering Department
  - Navy Cash – Supply Department

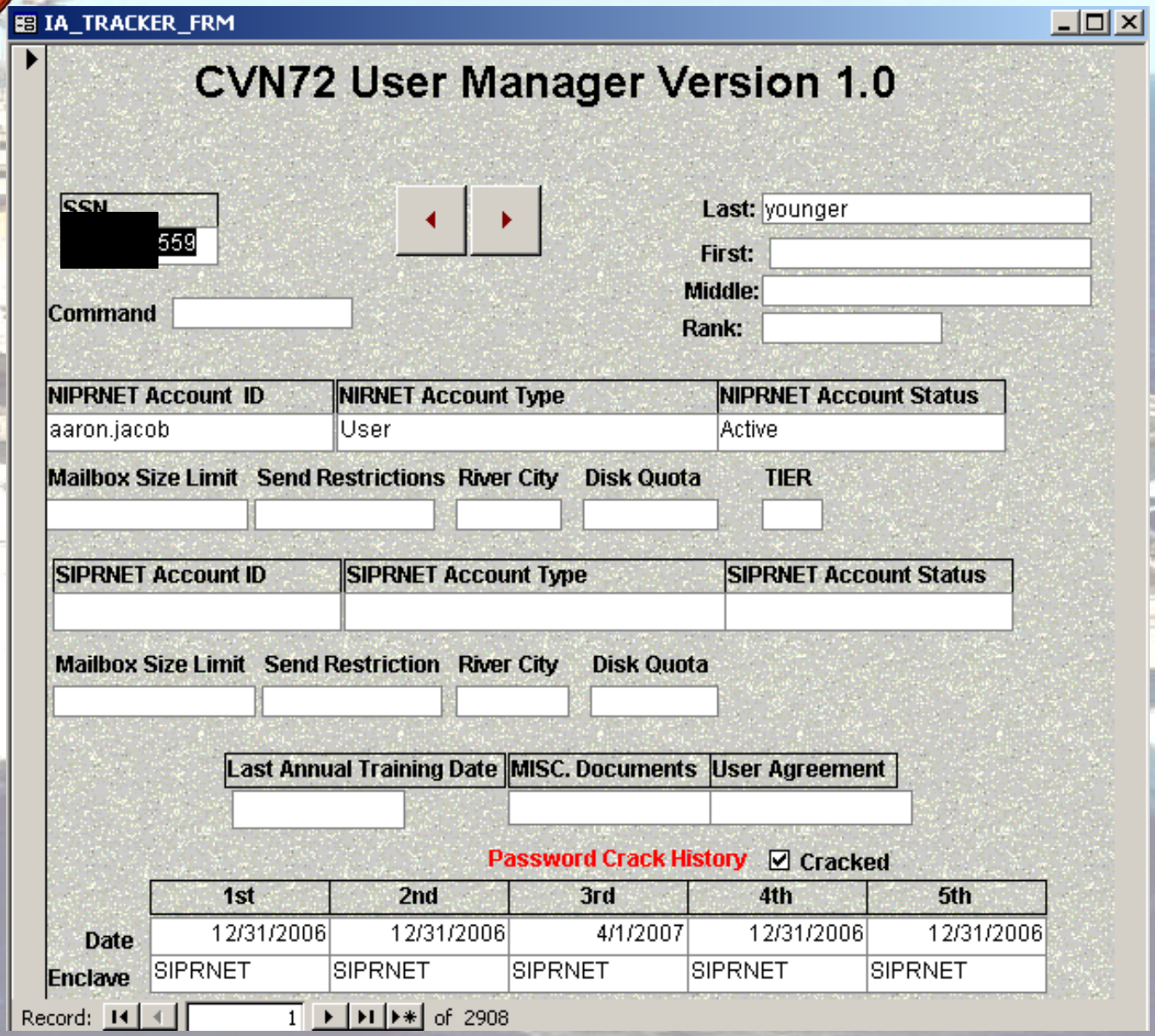
USS Abraham Lincoln CVN-72

Future Plans

Configuration Management

- Complete CM instructions
- Establish training plan to obtain civilian certifications
- Reduce man-hours consumed with inventory by requesting COTS package through the PPL/SSIL approval process
- Conduct port locking on switches
- Find or develop tools to reduce manpower required to monitor and maintain baseline configuration
- Complete user management database created by CVN 72

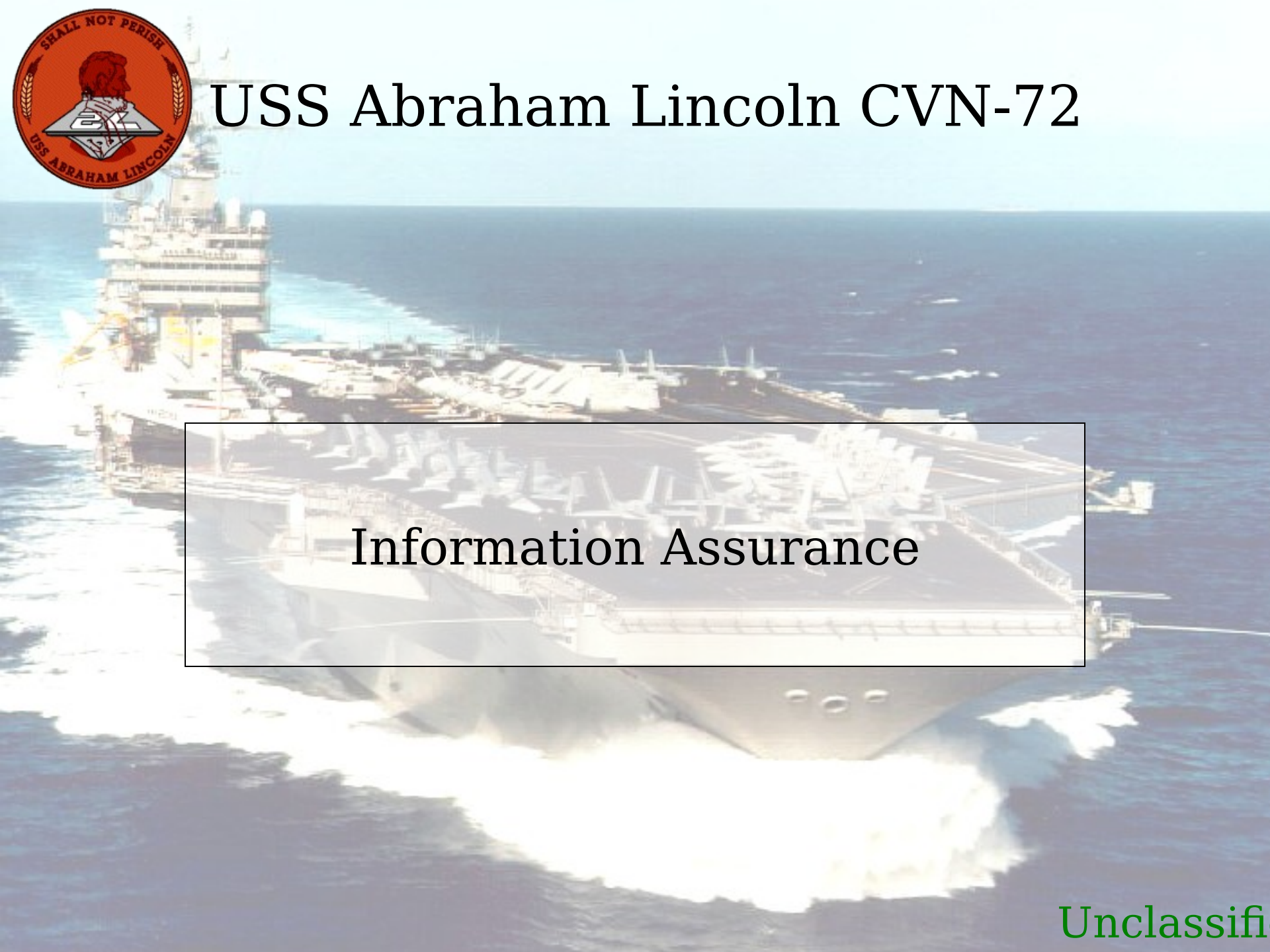
CVN72 User Manager



Unclassifi

Shipboard Training

- Develop user training curriculum to include:
  - Basic PC troubleshooting and solutions
    - Mapping network drives
    - Adding network printers
    - Basic housekeeping: Home Drive and Inbox management
  - Basic Microsoft desktop applications
    - Outlook
    - PowerPoint
    - Word
    - Excel
  - Information Security



USS Abraham Lincoln CVN-72

Information Assurance

Unclassifi

Information Assurance Division Who's Guarding the Hen house?

- Separate Operations and Customer Service from the Configuration Management (CM) and Information Assurance Vulnerability Management (IAVM)
  - Operations and Customer Service - Automated Information Systems Officer (AISO)
  - CM & IAVM – Information Assurance Manager (IAM)
- Create separate Information Assurance (IA) Division
  - Network Security
  - Command Asset Management

Pre-Existing Conditions

- Information Assurance
  - Lacked proactive approach to CND
  - User agreement forms and user training not tracked
  - IAVM not consistent between SIPRNET and NIPRNET
  - No set schedule for audits: web browsing, file content

Information Assurance Division

- Full Employment of Departmental/Divisional Information Assurance Officers (IAO)
  - Designation letter clearly identifying responsibilities to the IAM and Commanding Officer
  - Monthly Inventory
    - Hardware (computers, printers, etc)
    - Network Configuration (LAN Drop Inventory)
    - Software

Aggressive CND Router Configuration

- CVN72 employs default “deny” Access Control List (ACL) for systems and TCP/UDP ports
  - Router only allows incoming traffic on assets that need to “talk” to the outside world
    - DNS Server
    - Proxy Server
    - Exchange Server
    - Replication servers
- SPAWAR policy requires all other Program Mangers to utilize the proxy server for outside connectivity
  - Not being adhered to by Program Mangers (CAC, Disbursing)
  - Combat Systems forces installers to go through proxy server
- Extremely effective against Red Team activity
- Extremely effective in identifying port scans
  - CVN72 logs all rejected connections

Aggressive CND
CVN72 IA Cell

- 24/7 IA Cell
  - Single point of contact
- Methodically conduct vulnerability scanning of assets on the network.
  - Ensures the command that network assets are at the appropriate security level and settings are maintained.

Aggressive CND
CVN72 IA Cell

- Limited employment of Retina
  - Only using Retina
  - Daily discovery scans
  - Investigate “new” assets discovered
- Daily IA report providing the command visibility of network health and situational awareness. Daily report includes:
  - Viruses definitions status
  - Results of the daily password cracks
  - Results of inappropriate use of the Internet
  - Pending NCR with NCDOC
  - Pending IAVA/B actions
- Active blocking and researching of remote proxy web sites

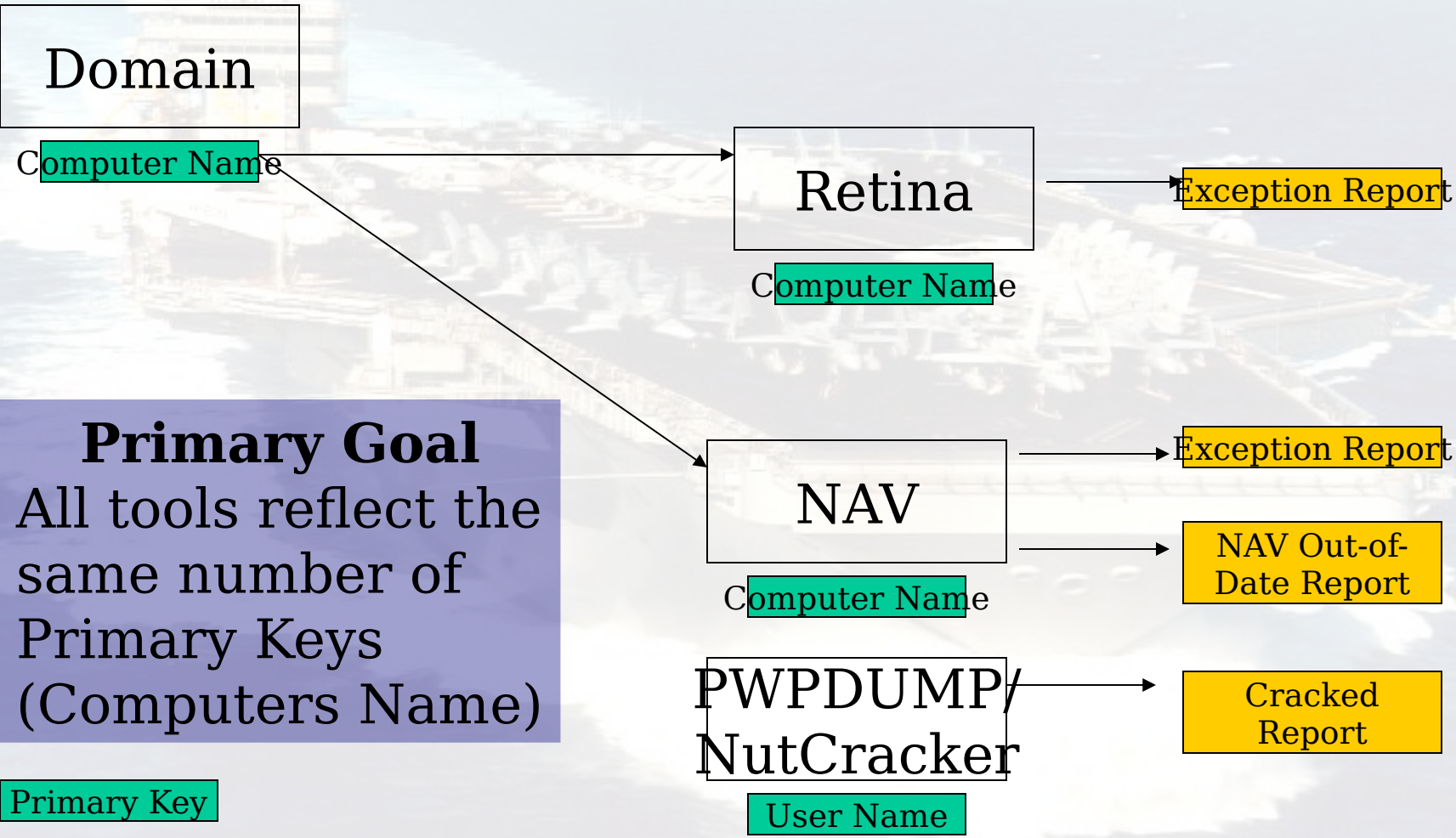
IA Division Successes

- Training accomplished & continuing
  - Watch Stander can process incident reports accurately
  - Watch Stander can report and direct required actions for information spills
  - Watch Stander can efficiently monitor and CND/IDS
- Have attained global situational awareness
- Identified and blocked over 1,200 remote proxy websites

Information Assurance Division

- Continue to develop policies and procedures
- Increase watch standers level of knowledge
- Establish training plan to obtain civilian certifications
- Expand IA Cell to include more robust network monitoring tools

IA Daily Report



Primary Goal

All tools reflect the same number of Primary Keys (Computers Name)

Primary Key

USS Abraham Lincoln CVN-72

Concerns & Issues

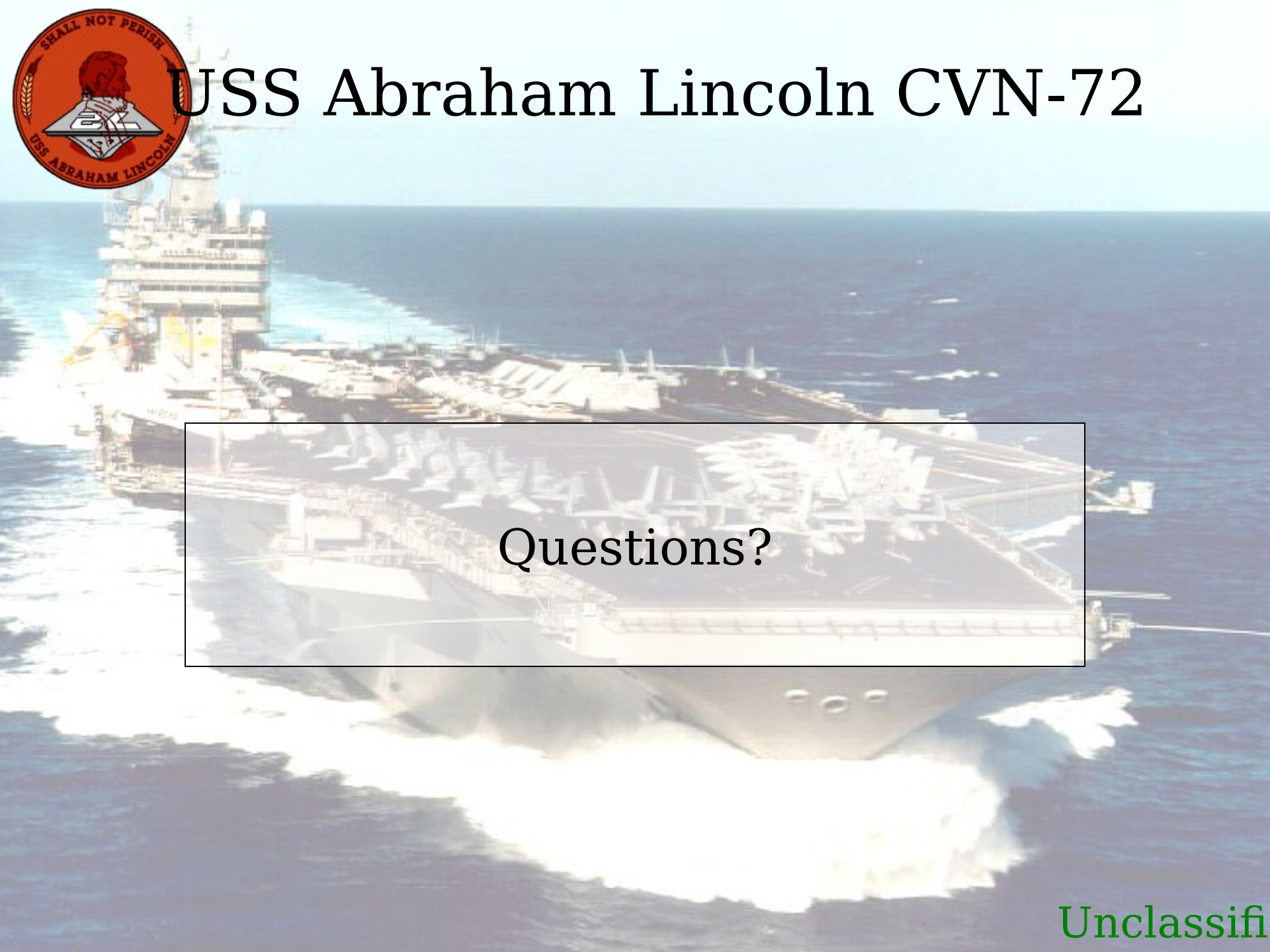
Web Browsing Policies

- Tools provided by standard ISNS configuration are inadequate to enforce DON policy on use of the Internet.
- CVN72 uses Microsoft Access to audit the proxy and Winsock proxy logs (requires 2 hours per audit).
- CVN72 employs the COTS product “Surf Control” to proactively monitor and control web browsing content.

End Point Security

- USB Removable Hard Drives and USB Thumb Drives
  - Not previous a concern on NIPRNET
  - DON Safeguard Personally Identifiable Information (PII) (NTD) 04-07.
  - No tool for enforcement
  - Required Hardware (Thumb Drives) on PPL/SSIL/QPL
- Effective 01 October 2007, storage of any form of PII is prohibited on personally owned computers (to include laptops), mobile computing devices and removable storage media.
  - No tool for enforcement

USS Abraham Lincoln CVN-72



Questions?

CVN 72 Contact Information

- CSO: CDR Scott Colton
  - cso@cvn72.navy.mil
- CSIO: LCDR Michelle Young
  - csio@cvn72.navy.mil
- CSMO: LCDR Greg Ludwig
  - csmo@cvn72.navy.mil
- IAM: LCDR Dave White (P-CSIO)
  - iam@cvn72.navy.mil
- ADP: ENS Adrian Young
  - adpo@cvn72.navy.mil